October 13, 2016

Ms. Marlene H. Dortch
Secretary
Federal Communications commission
445 12 Street, SW
Washington, DC 20554

Re: Protecting the Privacy of Customers of Broadband and Other Telecommunications Services, WC Docket No. 16-106

Dear Ms. Dortch:

The Internet Commerce Coalition (ICC) files this Ex Parte letter in the above proceeding in order to report a meeting between Jim Halpert and Sydney White of DLA Piper LLP (US) on behalf of the Internet Commerce Coalition with Claude Aiken, Wireline Advisor to Commissioner Clyburn on October 11, 2016. We focused on the following points: 1) the categories of sensitive information under the draft final order are inconsistent with the definition established by the FTC and the White House and 2) the consent requirements for sensitive and non-sensitive data should track the conclusions in the FTC's privacy framework.

Addition of Web Browsing and App Usage as Sensitive Information

During the meeting, we discussed the Protecting the Privacy of Customers of Broadband and Other Telecommunications NPRM and Chairman Wheeler's "Proposal to Give Broadband Consumers Increased Choice Over Their Personal Information". Specifically, Chairman Wheeler's Proposal released on October 6 would have the FCC adopt rules that treat contents of communications, web browsing data and app usage history as equally sensitive data for purposes of the FCC's final broadband privacy rules. If the FCC decides to include contents of communications as part of a category of sensitive information, it should not extend the same level of protection to "non-content" web browsing information and app usage history as these elements do not necessarily merit additional protections.

We discussed how a core feature of the privacy framework of the Obama Administration and the FTC has been technology-neutral requirements that provide strong, consistent privacy protections for consumers. This approach benefits consumers because it avoids confusing consumers about the extent to which their privacy is protected online through obscure variations in privacy rules based upon the type of business of the entities with which consumers conduct

business online. A consistent approach of the sort that the FTC Comments proposed would also avoid a First Amendment challenge based upon the rules providing a different approach for Internet advertising.

We discussed that the FTC Comments did not suggest that non-content web browsing or app usage information should be subject to an opt-in consent requirement, and including this requirement in the final order would create a very different rule for ISPs than the regime that applies for the rest of the Internet ecosystem.

Both the FTC and the body of the Electronic Communications Privacy Act ("ECPA") case law have examined the question of what qualifies as content, and in both cases it is well-established that neither URL addresses of Internet sites visited by a consumer, much less app usage data, are necessarily sensitive information that would require an opt-in consent requirement. And the FTC has determined that opt-out choice is appropriate for the use of all non-sensitive web browsing history, and this is the approach that applies throughout the Internet ecosystem today.

First Party Marketing

We discussed that privacy legislation does not regulate all information in a sector the same way when it enacts a sectoral privacy statute, and that Section 222 of the Communications Act does not reflect a Congressional judgment that all information handled by telecommunications carriers is sensitive. For example, Section 222 has an exception for "subscriber list information" which is not subject to the same protections as CPNI and which carriers are required to make publically available for competitive reasons. Likewise, ECPA also treats contents of communications and subscriber list information very differently, recognizing that the privacy interest in subscriber list information is lower than that in contents of communications.[1]

Finally, we discussed that Internet companies, including ISPs, have routinely implemented special protections so as to not target advertising or market to consumers on the basis of sensitive data categories, unless opt-in consent is obtained. This distinction is a key part of the Digital Advertising Alliance and Network Advertising Initiative self-regulatory frameworks, in which many Internet companies, including ISPs, participate. The participants are subject to enforcement, by government regulators and industry regulatory bodies, and the FCC would have even stronger enforcement levers to ensure compliance.

The final FCC rules should reserve opt-in consent for the elements of sensitive data identified by the FTC Comments and should otherwise apply the opt-out or implied consent approach set forth in the FTC's 2012 Privacy Report. For example, first-party marketing of an ISP's other products and services should be permissible based on implied consent, as both the FTC and Administration have previously concluded. Nor should the rules provide disparate treatment for the same online data depending upon which entity is collecting and using it. Instead, the notice requirements in the final rules could give consumers very clear information to

[1] Compare, e.g., 18 U.S.C. § 2511 with 18 U.S.C. § 2703(c).

empower them to decide whether to opt-out where implied consent does not apply, and that this information would better empower consumers than requiring opt-in consent for non-sensitive data.

Respectfully submitted,

/s/ **Sydney M. White**

Jim Halpert
Sydney M. White
Counsel to Internet Commerce Coalition